IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application Transmittal

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir: **10/29/98**

Date: October 29, 1998

Transmitted herewith for filing is the **Patent Application under Rule 53 (f)** of:

Inventor(s): Don Coppersmith, Claude A. Greengard, Charles P. Tresser and Chai Wah Wu

For: SYSTEM FOR PROTECTION OF GOODS AGAINST COUNTERFEITING

Enclosed are:

[X] Four (4) sheets of drawings. (INFORMAL)

[X] An assignment of the invention to International Busines Machines Corporation, Armonk, New York 10504.

[ ] A certified copy of a _____ application.

[X] Signed Declaration and Power of Attorney

[ ] Information Disclosure Statement with copies of cited references.   [X] Associate Power of Attorney

The filing fee has been calculated as shown below:

	(Col. 1)	(Col. 2)		Other Than Small Entity	
For:	No. Filed	No. Extra		Rate	Fee
Basic Fee					$ 790.00
Total Claims	21 -20 =	1		x $22.00=	$ 22.00
Indep. Claims	3 - 3 =	0		x $82.00=	$
[ ] Multiple Dependent Claim Presented				$270.00	$
				TOTAL	$ 812.00

[XX] ' Please charge Deposit Account No. 09-0468 in the amount of $812.00. A duplicate copy of this sheet is enclosed.

[XX] The Commissioner is hereby authorized to charge payment of the following fees associated with this communication or credit any overpayment to Deposit Account No. 09-0468. A duplicate copy of this sheet is enclosed.

[XX] Any additional filing fees required under 37 C.F.R. §1.1

[XX] Any patent application processing fees under 37 C.F.R. §1.17.

Respectfully submitted,

BY: _____
Attorney: Stephen C. Kaufman
Registration No.: 29,551 Tel.: (914) 945-3197

"EXPRESS MAIL" Label No. EL140119774
DATE OF DEPOSIT: October 29, 1998

SYSTEM FOR PROTECTION OF
GOODS AGAINST COUNTERFEITING

DESCRIPTION

BACKGROUND OF THE INVENTION

Cross-Reference to Related Applications

This application is a continuation-in-part (CIP) of co-pending application Serial No. 09/060,026, filed April 14, 1998. This application is related to Application Serial No. _____ filed October   , 1998 by A. Halperin et al (IBM Docket No. YO998-287) entitled "Method and System for Preventing Counterfeiting of High Price Wholesale and Retail Items"; and to Application Serial No._____ filed October   , 1998 by A. Afzali-Ardakani et al (IBM Docket No. YO998-342) entitled "Method and System for Preventing Parallel Marketing of Wholesale and Retail Items"; which related Applications are being filed contemporaneously with this application. The entire disclosure of each of these applications is incorporated by reference herein. Each of these three application is copending and commonly assigned.

Field of the Invention

The present invention generally relates to distinguishing authentic goods from counterfeit goods and, more particularly, to a system for authenticating consumer goods using an electronically authenticatable device attached to goods.

YO9-98-313   1

Description of the Related Art

Counterfeit or "knock-off" goods costs billions of dollars yearly to companies around the world in lost sales. Many counterfeited products are of inferior quality and therefore may tarnish the reputations of legitimate producers when consumers mistake the counterfeit for the real thing. Even if a counterfeit good is well done, the counterfeiter has avoided any of the expenditures in the research and development or intellectual property concerns incurred by or owed to the legitimate producer. Consumers and producers both suffer from counterfeiting through increased prices for legitimate merchandise and inferior quality of fraudulent merchandise.

Complete prevention against counterfeiting is probably unrealistic, at least for products which are manufactured. Some types of counterfeiting, often of inferior quality, are embraced by some consumers who desire to own, but cannot afford, expensive goods. Also, for products which are easily duplicable with no or little quality loss, some consumers prefer to protect their immediate financial interest rather than the interest of the legitimate producers.

Nevertheless, whether it be for the sake of honesty or because of quality concerns many, if not most, consumers prefer to purchase only authentic merchandise, especially when full price was paid. For these consumers, it is desired to provide a system by which the authenticity of a product can be confirmed to insure that what is being paid for is in fact the real thing.

It has been widely recognized by management of corporations most exposed to counterfeiting, such as, for example, manufacturers of compact disks (CDs), videos,

perfumes, luxury watches, etc., that allowing the public to verify the authenticity of a product with a high degree of certainty would substantially help to mitigate damages incurred from counterfeiters.

Many ingenious anti-counterfeit schemes have been devised over the years. A typical example of a system widely used to identify a counterfeit good involves the use of seals which have traditionally been used to authenticate documents. Variations on this theme include watermarks, such as are found on some international currencies, fine prints, tiny objects attached to a product or the package such as holograms, and so on. The efficacy of such methods has dramatically decreased with the evolution of technology. Due to progress in various technologies, if the customer can recognize the "seal", the counterfeiter usually can imitate it in such a way that the customer cannot detect the difference. For example, holographic seals verifiable by a consumer, once difficult and expensive to reproduce, are now child's play with relatively inexpensive equipment.

On the other hand, it is easy to produce seals only verifiable by the vendor. However, the cooperation of the consuming public to contact the vendor to verify the seal is a drawback. To partially overcome this difficulty, several manufacturers attach a serial number to each item. It has been proposed to improve on this method in U.S. Patent Number 4,463,250 to McNeight et al. and in U.S. Patent Number 5,367,148 Storch et al. For serial numbers to offer increased protection, these patents propose to use a serial number where part or all of the digits are chosen at random or generated by some secret code. The originator keeps a copy of all numbers so generated and the check of authenticity is performed by verifying that the tag of a

given item carries a number on the list. Such methods also propose some partial check using a small computer. Unfortunately, these methods suffer from several drawbacks. First, the need to contact the originator is unavoidable in the prior art. In such case, a counterfeiter may saturate the communication lines used for verification and make the process inefficient. Further, the fact that a database has to be kept of all purchases creates invasion of privacy issues for consumers. For example, if the consumer pays using a credit card, it becomes easy to attach the consumer's name to the product which has been bought, often without the consent of the consumer. Moreover, the originator must keep an ever growing database and must make this database quite secure for an unforeseen amount of time. Every access to the database must be secure, and one has to make certain that no external party obtains access to the database. This of course becomes increasingly difficult the larger and more often the data base is accessed. Secondly, using a small scanner, and the help of several accomplices, a would be counterfeiter may copy huge lists of existing serial numbers if the serial numbers are visible when the product is packaged, and the public has no means by which to even partially authenticate the product prior to purchase if the serial numbers are hidden. This problem is partially due to the fact that there is not very much connection between the serial number and the product it corresponds to, i.e. the serial number does not contain enough information about the product.

Another serious problem related to counterfeiting involves so called "parallel markets". There are two typical scenarios. In the first, stolen new goods can be reintroduced in various markets as genuine new goods, this

is commonly referred to as the "black market". In the second, sometimes referred to as the "grey market", a producer sells on different markets having different pricing policies. An agent in a lower priced market may resell the producer's goods to an agent in a higher priced market. In both cases, the producer loses.

SUMMARY OF THE INVENTION

It is therefore an object of the present invention to help protect legitimate vendors and the public against difficult to recognize counterfeits.

It is yet another object of the present invention to aid law enforcement authorities in the pursuit of counterfeiters and identifying illegal counterfeit goods as well as goods being sold in parallel markets.

It is yet another object of the present invention to provide a system for authenticating goods by using tamper-resistant and/or duplication-resistant electronic "tags" such as smart cards attached to goods.

According to the invention a smart tag attached to the goods contains encrypted authentication information, such as a serial number, and can further contain encrypted identifying information associated with the goods such as, for example, a description of the good's physical appearance or chemical decomposition, its color, its routing information, etc. The encryption procedure comprises public/private key encryption with zero-knowledge protocols. Zero knowledge protocols allow a smart tag to be authenticatable and yet be duplication resistant by allowing the verifying agent to convince him/herself that the smart tag is authentic without revealing its authentication

information.

The verification procedure can be done using a contact or contactless card reader equipped with the appropriate public key and zero-knowledge protocols to decrypt the

5   identifying information. A printed version of the serial number or other authentication information may be placed on the goods in human readable form to quickly verify the information electronically read from the smart tag. With the present invention, only the manufacturer can create such

10   smart tags with the associated data thus making it virtually impossible to pass off a counterfeit good as authentic.

BRIEF DESCRIPTION OF THE DRAWINGS

15   The foregoing and other objects, aspects and advantages will be better understood from the following detailed description of a preferred embodiment of the invention with reference to the drawings, in which:

Figure 1 is a block diagram of a first embodiment of

20   the present invention;

Figure 2 is a sample of a possible serial number structure according to the present invention;

Figure 3 is a block diagram of a second embodiment of the present invention; and

25   Figure 4 is a block diagram of an embodiment of the invention for identifying parallel markets.

DETAILED DESCRIPTION OF A PREFERRED
EMBODIMENT OF THE INVENTION

30

Referring now to the drawings, and more particularly to Figure 1 there is shown a block diagram of a first

embodiment of the present invention. A legitimate manufacturer 101 commands a serial number generator 102 to generate sequences of serial numbers. These serial numbers can be just consecutive numbers, or contain uncoded and/or

5 coded information as exemplified in Figure 2. The legitimate manufacturer 101 also possesses private keys, 103 and 104, and the corresponding public keys, 109 and 110, from private key/public key pairs as available now in many forms.

Public key encryption involves the use of
10 private/public key pairs. The private key is known only to the manufacturer. Using a corresponding public key provided by the manufacturer, the consumer or law enforcement agent can verify that the encrypted version matches the serial number. An advantage to this method is that only the
15 manufacturer can produce matching pairs. The wide spread availability of the public key does not compromise the security of the private key. The public key for verification can be made available on the product itself or by the manufacturer for example over the Internet. A comprehensive
20 description on the subject of private/public key pairs and zero-knowledge protocols can be found in "Handbook of Applied Cryptography", Alfred Menezes et al., CRC Press, 1997, and in "Cryptography: theory and practice", D. R. Stinson, CRC Press, 1995, herein incorporated by reference.

25 Zero knowledge protocols may be used to allow a smart tags to be authenticatable and yet be duplication resistant by allowing the verifying agent to convince him/herself that the smart tag is authentic without the smart tag revealing its authentication information. Such zero knowledge
30 protocols have been disclosed for instance in U. S. Patent 5,140,634 to Guillou et al., U.S. Patent 4,864,110 to Guillou, and U.S. Patent 4,995,082 to Schnorr, all herein

incorporated by reference.

Referring still to Figure 1, the serial number generated by generator 102 is encrypted using the private keys 103 and 104. The serial number and its encrypted version from 103 are communicated to printer-1 at block 105, while the encrypted versions from private key 104 is communicated to smart card writer at block 106. Printer 1 at block 105 prints a visible label 107 and the smart card writer at block 106 produces a smart card 108 containing the coded information prepared at 104. The visible label is attached to the product, while the smart card 108 is either attached to the product or simply packaged with the product. The legitimate manufacturer 101 make the public keys, 109 and 110, accessible to the customer or law enforcement agents 112, for instance through a link of the Internet World Wide Web (WWW) 111. The customer can verify authenticity in a first stage by examining the visible label using public key 109 or verification can be performed by the customer after the purchase by examining the hidden label using public key 110. The cashier may verify the authenticity of the product from the visible label in front of the customer with a point of sale (POS) machine 115 such as a cash register equipped with the appropriate public key and, if desired, a smart card reader.

The protection coming from the smart card containing the serial number and the private key/public key pair 104 and 110 can be omitted if the customer is satisfied with the level of authenticity verification provided by the visible label. Similarly, specific agents may only be interested verifying the smart card in which case the label can be omitted. Using the link to the WWW 111, or some other link to the legitimate originator, the customer may be able to

register the serial number of the product that has been
purchased. After the customer initiates such initial
contact, the manufacturer can contact the customer for
example to relay product update information, recall
5   information, etc.

The label and smart card composition and data can be
further detailed as follows for a series of serial numbers
with reference now to Figure 3. The product information 201,
manufacturing information 202, routing information 203, and
10   the previous serial number in the series (or some
initialization number at first stage) 204 are sent to the
serial number generator 205. The serial number is sent to
private key number-2 at block 206. The encrypted versions of
the serial number is sent to the smart card writer at block
15   209 which writes it on the smart card 211. The serial number
is also sent by the serial number generator 205 to printer-1
at block 208, possibly in conjunction with an encrypted
version of it, encrypted using private key number 1 at block
207. What is received at printer-1 208 is printed on the
20   visible label 210. Controls are be made, using the public
keys corresponding to private key-1, and if needed private
key- 2, to verify that the label and the smart card 211
correspond to each other and, when private key-1 is used,
that the readable and encoded versions of the serial number
25   match on the visible label. Private key-1 (207) can be
replaced by some apparatus generating a watermark or other
alteration of the product which do not affect its quality in
a human-perceptible way.

The visible label will be printed by a printer linked
30   to a computer 213. A part of the serial numbers is composed
in successive sequences incremented by one. A part of the
serial number will preferably contain information such as

routing, product name, date, etc. Each serial number is processed by two private key encoders, yielding two numerical identifiers. One of the numerical identifiers is written to the smart card while the serial number and the

5   second identifier are printed on the label, which will later be glued directly to the product or its packaging so as to be visible from the outside. The printing chain is also equipped with a verifier device (not shown) which checks that the various sets of numbers are printed in a

10   synchronous way. The second numerical identifier allows a preliminary check of authenticity, which should enable easy identification of the more flagrant counterfeit product labeling.

Instead of a serial number, the numerical identifier

15   could include a description of the physical appearance of the product, the color of the product, a chemical decomposition of the product and other descriptions of the product, including digital images of the product. This information will be contained in block 201 (Figure 3).

20   Furthermore, the identifier could also be encoded in various forms of widely used barcodes.

A smart tag may be a smart card 211 or any other electronic device which contains memory and/or processing and computation circuitry and can operate autonomously and

25   responds to queries from a verifying or authentication device. A more detailed discussion to smart card technology and applications can be found in "Smart Cards: a guide to building and managing smart card applications," by Henry Dreifus and J. Thomas Monk, John Wiley & Sons, 1998, herein

30   incorporated by reference.

In case zero-knowledge protocols are used the smart card 211 is tamper resistant and/or duplication-resistant.

For certain applications, the smart card 211 may be programmed to self-destruct (i.e., erases its contents) after verification in which case the use of a visible label may be dispensed with. Alternatively, it could be kept and maintained as a title and record of the whole resale history of the product to which it is attached. Depending on applications, the smart card can contain only authentication information showing that the attached goods came from the purported manufacturer. For instance, the smart card can contain authentication information about the manufacturer, not the particular goods themselves, in which case the smart card is the same for all products by the manufacturer. In other applications, the smart card can further contain specific encrypted information about the attached goods, such as digital images of the goods, a physical or chemical description of the goods, unique serial numbers, etc. The verification procedure can be done using a card reader 215 equipped with the appropriate public key and zero-knowledge protocols to decrypt the identifying information. The card reader 215 may be required to make contact with the card 211 or, in certain applications where the card 211 is embedded in the goods, inductive, capacitive or some other type of contactless coupling may be employed by the reader to read the card 211.

Referring to Figure 4, this invention can be used to prevent parallel markets from occurring by encoding routing information into the serial number or in the coded version of it. At the point of sale, the customer can ask to authenticate the product, and this verification can only be done if the routing information is kept intact, and is compatible with the actual point of sale. The smart card reader which performs this authentication is designed to

only function in such circumstances. For example, the manufacturer give each merchant the routing information encrypted with a private key and the smart card reader can only authenticate the product if decrypting the encrypted

5   routing information with a corresponding public key results in a match with the routing information on the product. In block 402, the smart card reader obtains the encrypted routing information from the merchant and decrypt it using a corresponding public key (403). In decision block 404 the

10   decrypted routing information is compared with the routing information in the smart card. If they do not match, the product is not meant to be sold here and the authentication fails. If they do match, in decision block 405 the smart card is authenticated. If the smart card is not

15   authenticated, the product fails to be authenticated. If the smart card is authenticated, in decision block 406, the product information in the smart card is compared with the serial number and/or other types of product information. If they do not match, the product is not authenticated. If

20   they do match, the product is authenticated. As an additional incentive for the customer to perform such verification, one can decide that the warranty on a product can only be activated if the product can be authenticated in this way at the point of sale. Upon activation, the customer

25   can choose to obtain a printed version of the warranty. If desired, the merchant can write onto a special memory section of the smart card the date and other information of the purchase.

　　　While the invention has been described in terms of a

30   preferred embodiment, those skilled in the art will recognize that the invention can be practiced with modification within the spirit and scope of the appended

claims.

CLAIMS

We claim:

1   1. A system for verifying the authenticity of a
2   manufactured product, comprising:
3   an electronic tag attached to one of said product
4   and product packaging, said electronic tag comprising
5   a memory for storing authentication information for
6   said product in encrypted form; and
7   a reader equipped with a decryption key for
8   reading said authentication information from said
9   electronic tag to verify that said product is
10   authentic.

1   2. A system for verifying the authenticity of a
2   manufactured product as recited in claim 1 wherein said
3   electronic tag is a smart card.

1   3. A system for verifying the authenticity of a
2   manufactured product as recited in claim 1 wherein said
3   electronic tag is embedded into one of said product and
4   product packaging product.

1   4. A system for verifying the authenticity of a
2   manufactured product as recited in claim 1 wherein said
3   authentication information is encrypted using a private
4   key and said reader decrypts said information using a
5   corresponding public key.

1   5. A system for verifying the authenticity of a
2   manufactured product as recited in claim 1 further

3 comprising a point of sale machine containing said
4 reader for authenticating said product in front of a
5 consumer prior to purchase of the product.

1 6. A system for verifying the authenticity of a
2 manufactured product as recited in claim 1 wherein said
3 reader comprises means for reading said electronic tag
4 without physically contacting said electronic tag.

1 7. A system for verifying the authenticity of a
2 manufactured product as recited in claim 1 wherein a
3 zero-knowledge protocol is used to make said
4 authentication information resistant to duplication.

1 8. A system for verifying the authenticity of a
2 manufactured product as recited in claim 1 wherein said
3 authentication information is directed to a
4 manufacturer of the product.

1 9. A system for verifying the authenticity of a
2 manufactured product as recited in claim 1 wherein said
3 authentication information is specific to the product.

1 10. A system for verifying the authenticity of a
2 manufactured product as recited in claim 1 further
3 comprising a label having the authentication
4 information printed thereon to be verified against the
5 authentication information read by said reader.

1 11. A system for verifying the authenticity of a
2 manufactured product as recited in claim 9 wherein said
3 authentication information comprises one or more of

4   product color, product shape, product serial number,

5   product weight, product routing information, and

6   product chemical composition.

1   12. A system for verifying the authenticity of a

2   manufactured product as recited in claim 9 wherein said

3   authentication information comprises a graphic image of

4   the product.

1   13. A system for verifying the authenticity of a

2   manufactured product as recited in claim 9 wherein said

3   authentication information comprises an ownership

4   history of the product.

1   14. A system for verifying the authenticity of a

2   manufactured product as recited in claim 1 wherein said

3   authentication information is erased from said memory

4   after being read.

1   15. A system for verifying the authenticity of a

2   manufactured product as recited in claim 1 wherein said

3   authentication information further comprises

4   information for authenticating said electronic tag.

1   16. A method for verifying the authenticity of a

2   manufactured product, comprising the steps of:

3   generating authentication information for a

4   manufactured product;

5   encrypting said authentication information using a

6   private key;

7   storing said encrypted information in electronic

8   tag;

9   attaching said electronic tag to one of said

10   manufactured product and manufactured product

11   packaging;

12   reading said encrypted authentication information

13   from said electronic tag; and

14   decrypting said encrypted information using a

15   public key corresponding to said private key to verify

16   that said manufactured product is authentic.

1   17. A method for verifying the authenticity of a

2   manufactured product as recited in claim 16 further

3   comprising the step of using a zero-knowledge protocol

4   to make said authentication information resistant to

5   duplication.

1   18. A method for verifying the authenticity of a

2   manufactured product as recited in claim 16 further

3   comprising the step of attaching a printed label to

4   said product comprising said authentication

5   information.

1   19. A method for verifying the authenticity of a

2   manufactured product as recited in claim 16 further

3   comprising the step of erasing said authentication

4   information from said electronic tag after reading.

1   20. A method for verifying the authenticity of a

2   manufactured product as recited in claim 16 further

3   comprising the step of recording an ownership history

4   of said product in said electronic tag.

1   21. A method for detecting manufactured products in a

2   parallel market, comprising the steps of:
3   generating authentication information for a
4   manufactured product including routing information for
5   the product;
6   encrypting said authentication information using a
7   private key;
8   storing said encrypted information in electronic
9   tag;
10   attaching said electronic tag to one of the
11   manufactured product and manufactured product
12   packaging;
13   reading said encrypted authentication information
14   from said electronic tag at a point of sale; and
15   decrypting said encrypted information using a
16   public key corresponding to said private key to verify
17   said routing information matches routing information of
18   said point of sale to determine if said manufactured
19   product is sold in a parallel market.

ABSTRACT OF THE DISCLOSURE

In order to verify the authenticity of manufactured goods, a smart tag is attached to the goods containing encrypted authentication information, such as a serial number, a description of the good's physical appearance or chemical decomposition, its color, or digital images of the good etc. The encryption procedure comprises public/private key encryption with zero-knowledge protocols. Zero knowledge protocols allow a smart tag to be authenticatable and yet be duplication resistant by allowing the verifying agent to convince him/herself that the smart tag is authentic without revealing its authentication information. The verification procedure can be done using a reader at a point of sale (POS) machine equipped with the appropriate public key and zero-knowledge protocols to decrypt the authentication information. A printed version of the serial number or other authentication information may be placed on the goods in human readable form to quickly verify the information electronically read from the smart tag. With the present invention, only the manufacturer can create such smart tags with the associated data thus making it virtually impossible to pass off a counterfeit good as authentic. In addition to authenticating counterfeit goods, the present invention can be used to detect authentic goods being sold in a parallel market.

Figure 1
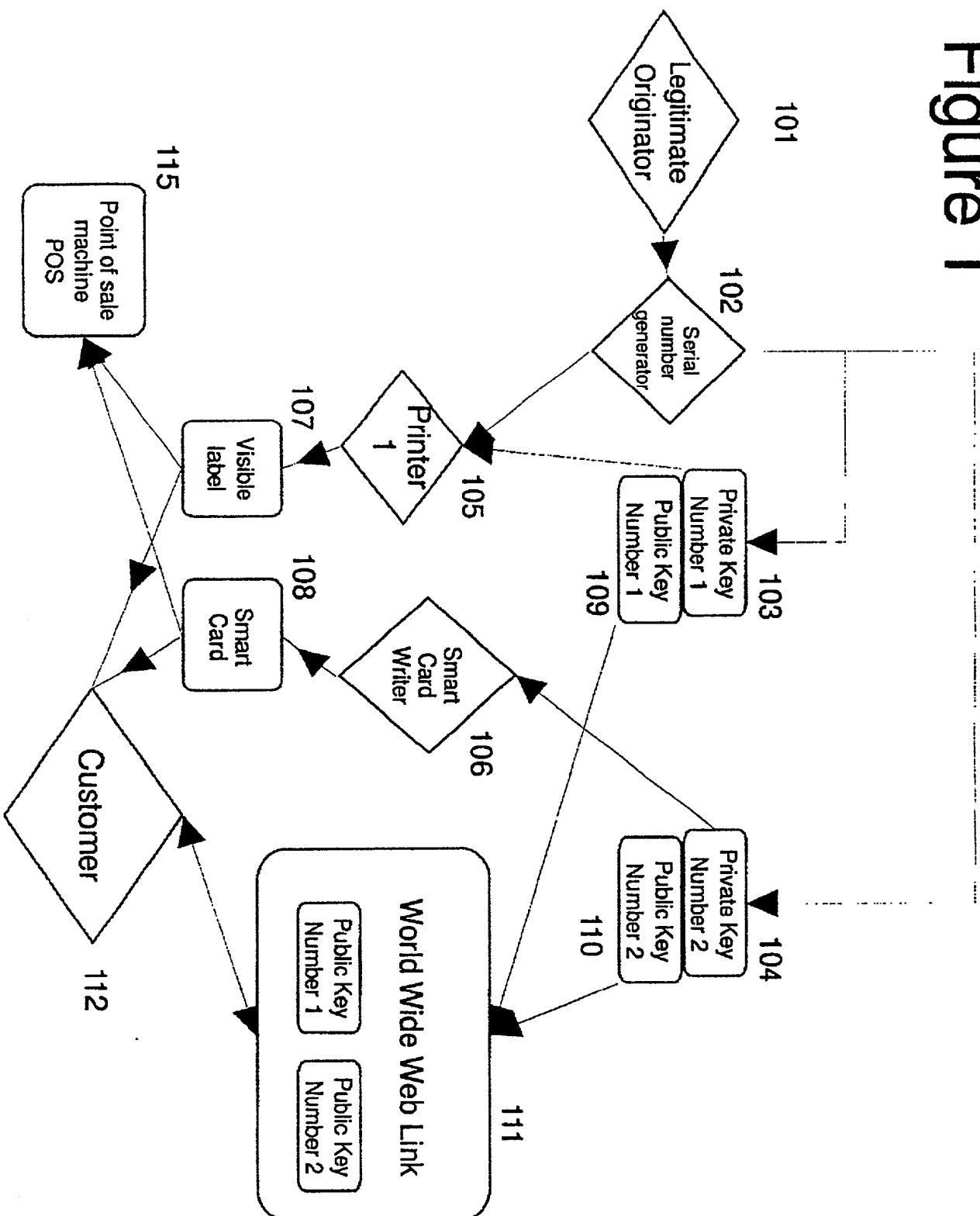
Carmen-Bizet-Xtaer12 ae34mnv56pil87lok56 wer56iol09pYT-njhg8 19837547542797874 green-circular-15oz	Complete serial number
Carmen-Bizet-	Product identifier
Xtaer12	Manufacturing information *
ae34mnv56pil87lok56 wer56iol09pYT-njhg8	Routing Information*
19837547542797874	Pure serial number
green-circular-15oz	Other product information

Sample serial number structure: the * items can be understandable or not by the customer

Figure 2

201 — Product Information

202 — Manufacturing Information

203 — Routing Information

204 — Previous serial number or initialization

205 — Serial number generator

206 — Private Key Number 2

207 — Private Key Number 1

208 — Printer 1

209 — Smart card writer

210 — Visible label

211 — Smart card

213 — Computer

215 — reader

Figure 3

Start

401

Obtain encrypted
routing
information from
merchant

402

Decrypt using
public key

403

Does decrypted
routing information
corresponds to
routing information
on smart card?

404

no → Product should not be
sold here: product is not
authenticated

yes

Is the smart
card
authenticated?

405

no → Product is not
authenticated

yes

Does the content of the
smart card corresponds to
the serial number on
product and/or product
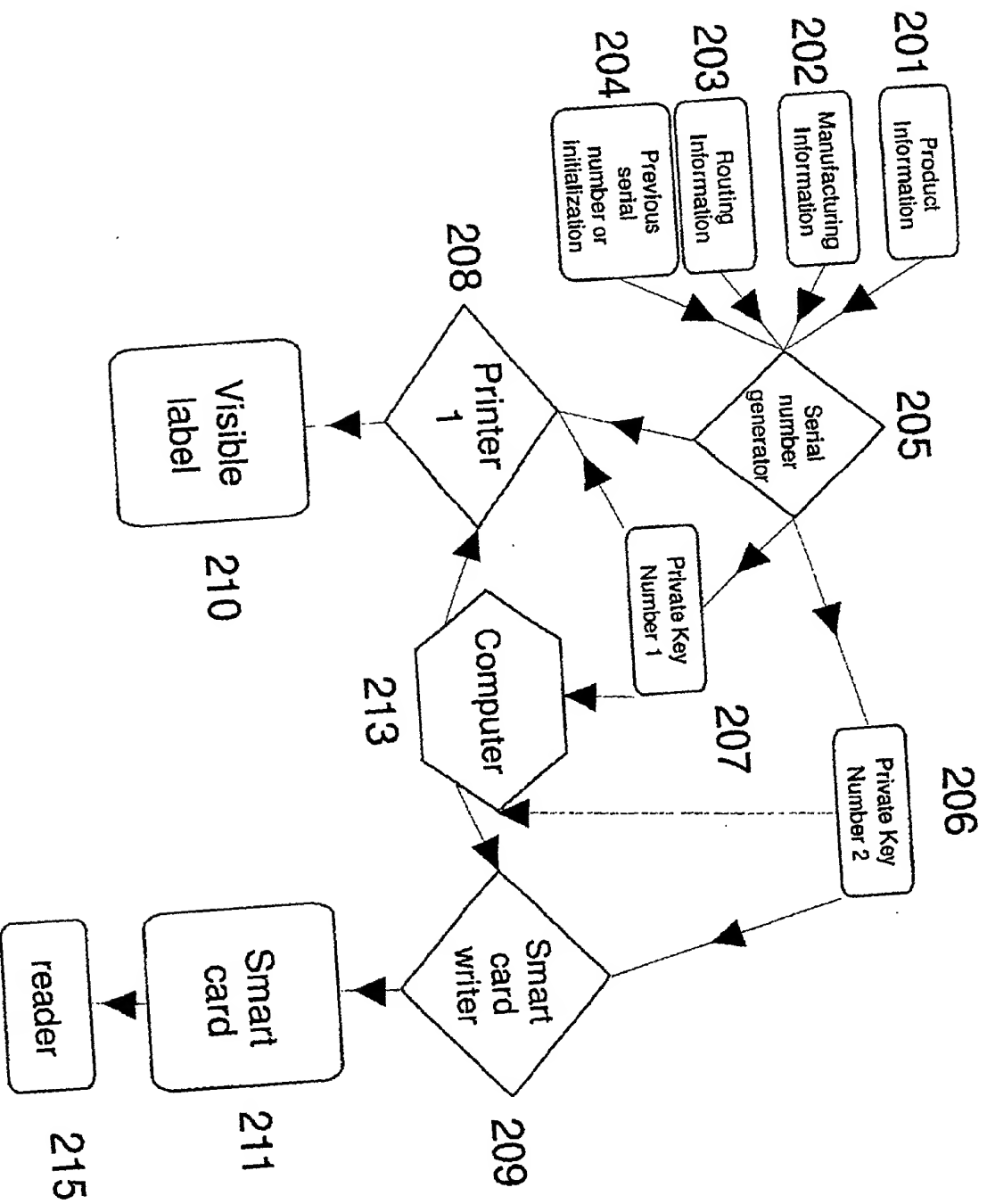information?

406

no → Product is not
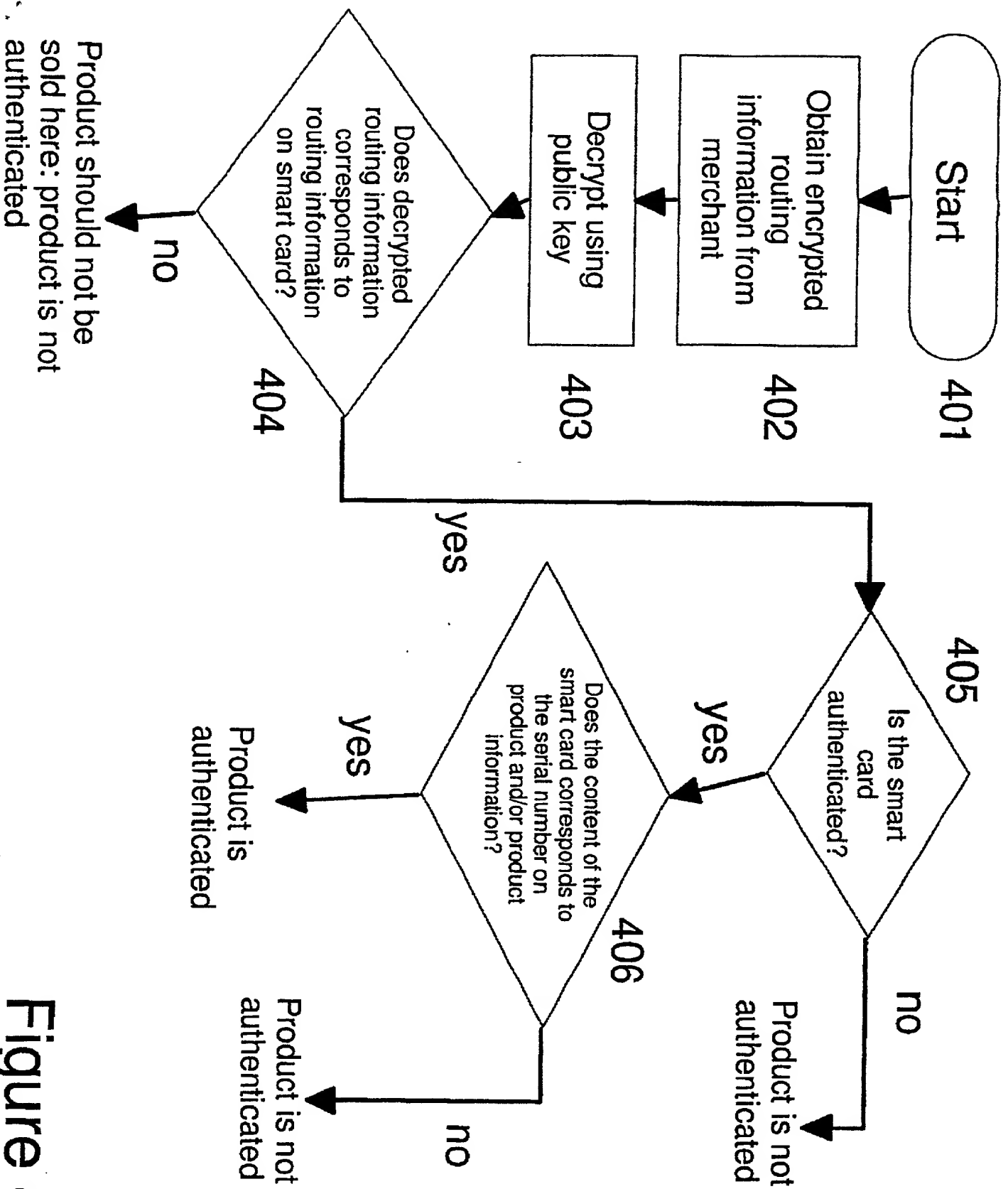authenticated

yes → Product is
authenticated

Figure 4

Docket No. YO998-313

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name;

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

SYSTEM FOR PROTECTION OF GOODS AGAINST COUNTERFEITING

the specification of which (check one)

_X_ is attached hereto.

____ was filed on _____ as United States Application Number _____

      or PCT International Application Number _____
      and was amended on _____ (if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §119(a)-(d) or §365(b) of any foreign application(s) for patent or inventor's certificate, or §365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or PCT International application, having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)   Priority Claimed

(Number)	(Country)	(Day/Month/Year Filed)	____ Yes ____ No
(Number)	(Country)	(Day/Month/Year Filed)	____ Yes ____ No
(Number)	(Country)	(Day/Month/Year Filed)	____ Yes ____ No

I hereby claim the benefit under 35 U.S.C. §119(e) of any United States provisional application(s) listed below.

(Application Number)	(Filing Date)
(Application Number)	(Filing Date)

I hereby claim the benefit under 35 U.S.C. §120 of any United States Application(s), or §365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States, or PCT International application in the manner provided by the first paragraph of 35 U.S.C. §112, I acknowledge the duty to disclose information material to the patentability of this application as defined in 37 CFR §1.56 which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

09/060,026	4/14/98	Pending CIP
(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)
(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: As a named inventor I hereby appoint Manny W. Schecter, Reg. 31,722, Terry P. Ilardi, Reg. 29,936, Stephen C. Kaufman, Reg. No. 29,551, Louis J. Percello, Reg. No. 33,206, Jay P. Sbrollini, Reg. No. 36,266, Robert M. Trepp, Reg. No. 25,933, Daniel P. Morris, Reg. No. 32,053, Kevin M. Jordan, Reg. No. 40,277, Douglas W. Cameron, Reg. No. 31,596, David M. Shofi, Reg. No. 39,835, Christopher A. Hughes, Reg. 26,914, Edward A. Pennington Reg. 32,588, John E. Hoel, Reg. 26,279, Joseph C. Redmond, Jr., Reg. 18,753, C. Lamont Whitham, Reg. No. 22,424, Marshall M. Curtis, Reg. No. 33,138, and Michael E. Whitham, Reg. No. 32,635, as attorneys and/or agents to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.

Send Correspondence to: __Whitham, Curtis & Whitham, Reston International Center__

_____11800 Sunrise Valley Drive, Suite 900, Reston, Virginia 20191_____

Direct Telephone Calls to: (name and telephone number)__Whitham, Curtis & Whitham, at 703/391-2510___

__Don Coppersmith__
Full name of sole or first inventor

Inventor's Signature	Date

__56 Ferris Place, Ossining, New York 10562__
Residence

__USA__
Citizenship

__Same as above__
Post Office Address

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

 Claude A. Greengard
Full name of second joint-inventor, if any

_____
Inventor's signature   Date

 40 Jeffrey Lane, Chappaqua, New York   10514
Residence

 USA
Citizenship

 Same as above
Post Office Address

 Charles P. Tresser
Full name of third joint-inventor, if any

_____ 10/29/98
Inventor's signature   Date

 953 West Boston Post Road, Apt. 2K, Mamaroneck, New York   10543
Residence

 France
Citizenship

 Same as above
Post Office Address

 Chai Wah Wu
Full name of fourth joint-inventor, if any

_____ 10-29-98
Inventor's Signature   Date

 66 Orchard Drive, Poughquag, New York   12570
Residence

 Netherlands
Citizenship

 Same as above
Post Office Address

Full name of fifth joint inventor, if any

_____
Inventor's Signature   Date

Residence

Citizenship

Post Office Address

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: D. Coppersmith et al   Dated: October 29, 2998
Serial No.:   Examiner:
Filed: HEREWITH   Docket No. YO998-313

For: SYSTEM FOR PROTECTION OF GOODS AGAINST COUNTERFEITING

APPOINTMENT OF ASSOCIATE ATTORNEY

The Commissioner of Patents and Trademarks
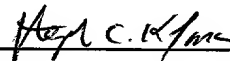Washington, D.C. 20231

Sir:

The undersigned attorney, who has been appointed as an attorney in the Combined Declaration and Power of Attorney for the above-identified application, hereby appoints C. Lamont Whitham (Reg. No. 22,424), Marshall M. Curtis (Reg. No. 33,138), and Michael E. Whitham (Reg. No. 32,635) of Whitham, Curtis & Whitham, Reston International Center, 11800 Sunrise Valley Dr., Suite 900, Reston, Virginia 22091 [telephone number (703) 391-2510] his associate attorney to prosecute said application and to transact all business in the Patent and Trademark Office connected therewith.

Please direct all official communications to:

> Whitham, Curtis & Whitham
> Reston International Center
> 11800 Sunrise Valley Dr., Suite 900
> Reston, Virginia 22091
> (703) 391-2510

Respectfully submitted,

Stephen C. Kaufman
Reg. No. 29,551
Tel. No. (914) 945-3197

IBM Corporation
Intellectual Property Law
P.O. Box 218
Yorktown Heights, N.Y. 10598
IBM Docket No.: YO998-313